Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.-2. (Canceled)

3. (Currently Amended) A method in a computer system for automatically protecting data stored in a portion of a storage device having a designated protected space, the computer system having a designated unprotected space and a redirected space, comprising:

loading a software redirection driver into an input/output driver hierarchy loaded in a volatile memory of the computer system during power-up initialization, wherein the software redirection driver is an input/output driver; and

under control of code of the loaded software redirection driver, redirecting input/output requests by:

intercepting from requesting code that is external to the loaded software redirection driver a request to modify a location in the protected space or a location in the unprotected space;

when the request is to modify a location in the unprotected space, initiating modification of the location in the unprotected space without redirection;

when the request is to modify a location in the protected space,

determining a location in the redirected space that is associated with the location in the protected space; and

redirecting the intercepted request to modify the determined location in the redirected space instead of the location in the protected space;

in response to a received request to shutdown the computer system, disregarding the data in the redirected space;

after the disregarding of the data in the redirected space, intercepting from requesting code a request to read the location in the protected space; and

in response to the intercepting of the request to read the location in the protected space, providing data from the location in the protected space instead of providing data from the redirected space, so that the data stored in the location in the protected space automatically remains unaltered when the computer system is restarted from a powered-down state.

4. (Original) The method of claim 3 wherein a redirection driver performs the intercepting the request, determining the location in the redirected space, and redirecting the intercepted request.

5. (Original) The method of claim 4 wherein the driver is inserted into a driver hierarchy that is controlled by an operating system of the computer system.

6. (Original) The method of claim 3 wherein the designated protected space of the storage device comprises the entire storage device.

7. (Original) The method of claim 3 wherein the determined location in the redirected space resides in the storage device.

8. (Original) The method of claim 3 wherein the determined location in the redirected space resides in an other storage device.

9. (Previously Presented) The method of claim 3, further comprising:

intercepting from requesting code a request to read the location in the protected space of the storage device;

determining the location in the redirected space that is associated with the location in the protected space; and

automatically redirecting the intercepted request to read from the determined location in the redirected space instead of from the location in the protected space in a manner that is transparent to the requesting code.

10. (Canceled)

11. (Previously Presented) The method of claim 3 wherein the request to modify the location in the protected space is a request to write to the protected space.

12. (Canceled)

13. (Original) The method of claim 11 wherein the redirecting the intercepted write request results in automatically allocating available space to use as new redirected space and writing data to a location in the new redirected space.

14. (Original) The method of claim 3 wherein the determining the location in the redirected space that is associated with the location in the protected space further comprises first allocating available space to be used as the redirected space.

15. (Previously Presented) The method of claim 3 wherein the storage device is one of a hard disk drive, a read/write CD ROM drive, a floppy disk drive, or a semi-persistent storage device.

16. (Previously Presented) The method of claim 3 wherein the location in the protected space refers to at least one of a sector, a group of sectors, a cluster, or a group of clusters.

17. (Previously Presented) The method of claim 3 wherein the location in the redirected space refers to at least one of a sector, a group of sectors, a cluster, a group of clusters, a virtual cluster, or a group of virtual clusters.

18. (Original) The method of claim 17 wherein the sector is a logical sector.

19. (Original) The method of claim 17 wherein the sector is a physical sector.

20. (Original) The method of claim 17 wherein the location in the protected space refers to a sector.

21. (Original) The method of claim 17 wherein the location in the protected space refers to an abstraction of storage that is larger than a sector.

22. (Previously Presented) The method of claim 3 wherein the redirected space is organized according to a combination of different storage abstractions.

23. (Previously Presented) The method of claim 22 wherein a portion of the redirected space is organized as one of virtual clusters, clusters, files, and sectors, and an other portion is organized according to a different storage abstraction.

24-25. (Canceled)

26. (Previously Presented) The method of claim 3 wherein the disregarding of the data in the redirected space comprises at least one of deleting the data from the storage in the redirected space, disassociating the redirected space from the protected space, or ignoring the data in the redirected space.

27-29. (Canceled)

30. (Original) The method of claim 3, further comprising using redirection tables to associate locations in the protected space to locations in the redirected space.

31. (Previously Presented) The method of claim 30 wherein the redirection tables comprise at least one of a protected space redirection table, an available space table, or an unprotected space table.

32. (Currently Amended) A computer-readable memory medium containing program code that controls a computer processor to protect data stored in a portion of a storage device having a designated protected space, the computer system having a designated unprotected space and a redirected space, by performing a method comprising:

loading a software redirection driver into an input/output driver hierarchy loaded in a volatile memory of the computer system during power-up initialization, wherein the software redirection driver is an input/output driver; and

under control of code of the loaded software redirection driver, redirecting input/output requests by:

intercepting from requesting code that is external to the loaded software redirection driver a request to modify a location in the protected space or a location in the unprotected space;

when the request is to modify a location in the unprotected space, initiating modification of the location in the unprotected space without redirection; and

when the request is to modify a location in the protected space,

determining a location in the redirected space that is associated with the location in the protected space; and

redirecting the intercepted request to modify the determined location in the redirected space instead of the location in the protected space,

in response to a received request to shutdown the computer system, disregarding the data in the redirected space;

after the disregarding of the data in the redirected space, intercepting from requesting code a request to read the location in the protected space; and

in response to the intercepting of the request to read the location in the unprotected space, providing data from the location in the protected space instead of providing data from the redirected space, so that the data stored in the location in the protected space automatically remains unaltered when the computer system is restarted from a powered-down state.

33. (Original) The computer-readable memory medium of claim 32 wherein the designated protected space of the storage device comprises the entire storage device.

34. (Original) The computer-readable memory medium of claim 32 wherein the determined location in the redirected space resides in the storage device.

35. (Original) The computer-readable memory medium of claim 32 wherein the determined location in the redirected space resides in an other storage device.

36. (Previously Presented) The computer-readable memory medium of claim 32, the method further comprising:

prior to the disregarding of the data in the redirected space,

intercepting from requesting code a request to read the location in the protected space of the storage device;

determining the location in the redirected space that is associated with the location in the protected space; and

automatically redirecting the intercepted request to read from the determined location in the redirected space instead of from the location in the protected space in a manner that is transparent to the requesting code.

37. (Previously Presented) The computer-readable memory medium of claim 32 wherein the request to modify the location in the protected space is a request to write to the protected space that results in automatically writing data to the determined location in the redirected space instead of to the location in the protected space.

38. (Original) The computer-readable memory medium of claim 37 wherein the redirecting the intercepted write request results in automatically allocating available space to use as new redirected space and writing data to a location in the new redirected space.

39. (Original) The computer-readable memory medium of claim 32 wherein the determining the location in the redirected space that is associated with the location in the protected space further comprises first allocating available space to be used as the redirected space.

40. (Previously Presented) The computer-readable memory medium of claim 32 wherein the storage device comprises one of a hard disk drive, a read/write CD ROM drive, a floppy disk drive, or a semi-persistent storage device.

41. (Previously Presented) The computer-readable memory medium of claim 32 wherein the location in the protected space refers to at least one of a sector, a group of sectors, a cluster, or a group of clusters.

42. (Previously Presented) The computer-readable memory medium of claim 32 wherein the location in the redirected space refers to at least one of a sector, a group of sectors, a cluster, a group of clusters, a virtual cluster, or a group of virtual clusters.

43. (Original) The computer-readable memory medium of claim 42 wherein the location in the protected space refers to a sector.

44. (Original) The computer-readable memory medium of claim 42 wherein the location in the protected space refers to an abstraction of storage that is larger than a sector.

45. (Previously Presented) The computer-readable memory medium of claim 32 wherein the redirected space is organized according to a combination of different storage abstractions.

46. (Previously Presented) The computer-readable memory medium of claim 45 wherein a portion of the redirected space is organized as at least one of virtual clusters, clusters, files, and sectors, and an other portion is organized according to a different storage abstraction.

47-48. (Canceled)

49. (Previously Presented) The computer-readable memory medium of claim 32 wherein disregarding the data in the redirected space comprises at least one of deleting the data from the storage in the redirected space, disassociating the redirected space from the protected space, or ignoring the data in the redirected space.

50-52. (Canceled)

53. (Original) The computer-readable memory medium of claim 32, further comprising using redirection tables to associate locations in the protected space to locations in the redirected space.

54. (Currently Amended) A computer system for automatically protecting data stored in a portion of a storage device, comprising:

a protected space on the storage device for storing the protected data;

an unprotected space;

redirected storage space in the computer system designated for storing attempted modifications of the protected data; and

a software redirection driver that redirects input/output requests, loaded into an input/output driver hierarchy loaded in a volatile memory of the computer system when the system is booted from a powered-down state, wherein the software redirection driver is an input/output driver including code that, when executed, is configured to:

intercept from requesting code that is external to the software redirection driver a request to modify a location in the protected space or a location in the unprotected space;

when the request is to modify a location in the unprotected space, initiate modification of the location in the unprotected space without redirection;

when it is determined that the request is to modify a location in the protected space, redirect the request so that the request results in modifying a location in the redirected storage space instead of the location in the protected space;

in response to a received request to shutdown the computer system, disregarding the data in the redirected space;

after the disregarding of the data in the redirected storage space, intercepting from the requesting code a request to read the location in the protected space; and

in response to the intercepting of the request to read the location in the protected space, providing data from the location in the protected space instead of providing data from the redirected space, so that the location in the protected space automatically remains unaltered when the computer system is restarted from a powered-down state.

55. (Canceled)

56. (Original) The computer system of claim 54, further comprising a redirection table that maps locations in the protected space to locations in the redirected storage space, and is used by the redirection driver to determine a location in the redirected storage space to use for redirecting an intercepted request.

57. (Original) The computer system of claim 56 wherein the contents of the redirection table are saved by the computer system when the computer system is powered down.

58. (Original) The computer system of claim 54 wherein the protected space comprises the entire storage device and the redirected storage space is not located on the storage device.

59. (Original) The computer system of claim 54 wherein the redirected storage space is located on the storage device.

60. (Original) The computer system of claim 54 wherein an intercepted and redirected access request is a request to read from a location in the protected space.

61. (Original) The computer system of claim 54 wherein an intercepted and redirected access request is a request to write to a location in the protected space that is redirected to modify a location in the redirected space.

62. (Previously Presented) The computer system of claim 54 wherein the storage device is one of a hard disk drive, a read/write CD ROM drive, a floppy disk drive, or a semi-persistent storage device.

63. (Previously Presented) The computer system of claim 54 wherein the redirection driver refers to the redirected storage space in at least one of files, clusters, virtual clusters, or sectors of data.

64. (Original) The computer system of claim 54 wherein the redirection driver refers to the redirected storage space using multiple data addressing abstractions.

65. (Original) The computer system of claim 54 wherein the redirection driver implements a virtual cluster data abstraction.

66. (Previously Presented) The computer system of claim 54 wherein the redirection driver is loaded by inserting the redirection driver into a chain of drivers so that it is automatically invoked by the computer system.

67-69. (Canceled)

70. (Previously Presented) The computer system of claim 54, further comprising an unprotected space table for tracking the locations of the storage device that are designated as unprotected space.

71. (Original) The computer system of claim 54 wherein the contents of the redirected storage space are saved by the computer system when the computer system is powered down.

72. (Previously Presented) A method for protecting data in a storage device of a computer system having an operating system, a device driver, an unprotected space, and a storage device having a designated protected space, comprising:

loading a software redirection driver into a volatile memory of the computer system during power-up initialization;

installing the software redirection driver before the device driver in a calling sequence of the operating system, so that the operating system invokes the redirection driver in response to receiving a request to access the storage device;

under control of the redirection driver,

intercepting from requesting code that is external to the redirection driver a request to modify a location referred to by a protected space redirection table or a location referred to by an unprotected space table;

when the request is to modify a location referred to by the unprotected space table, initiating modification of the location in the unprotected space without redirection; and

when the request is to modify a location referred to by the protected space redirection table, redirecting the request to modify a location in unused storage associated with the location referred to by the protected space redirection table, such that the data in the location in the protected space remains unaltered;

in response to a received request to shutdown the computer system, disregarding data in the location in the unused storage;

after the disregarding of the data in the location in the unused storage, intercepting from the requesting code a request to read the location in the protected space; and

in response to the intercepting of the request to read the location in the protected space, providing data from the location in protected space instead of providing data from the location in the unused storage, so that the data stored in the location in the protected space automatically remains unaltered when the computer system is restarted from a powered-down state.

73. (Original) The method of claim 72 wherein the redirection driver cannot be uninstalled by a user without special access privileges, thereby forcing the data to be securely maintained.

74. (Original) The method of claim 72, the device driver comprising one of a plurality of device drivers that are arranged in a layered fashion, and wherein the redirection driver is installed between two of these device drivers.

75. (Original) The method of claim 74 wherein each driver layer comprises a driver that communicates with an associated device according to different data abstraction; and wherein the redirection driver can be configured to be installed at different layers depending upon the data abstraction implemented by the redirection driver.

76. (Previously Presented) The method of claim 72 wherein the redirection driver handles blocks of data defined as at least one of virtual clusters, clusters, sectors, or files.

77. (Original) The method of claim 72 wherein the redirection driver handles multiple different data abstractions.

78. (Previously Presented) The method of claim 72 wherein the computer system comprises redirection tables that are maintained by the redirection driver to manage associations between data that has been redirected by redirecting the request to the location in unused storage and unaltered data stored on the storage device.

79. (Previously Presented) A storage access redirection system for protecting data in designated locations on a storage device in a computer system, the storage device having a designated unprotected space, the computer system having an unprotected space, comprising:

an available space table;

a protected space redirection table that is used to designate protected locations on the storage device that are to be protected from modification;

an unprotected space table that is used to designate unprotected locations on the storage device that can be altered; and

a software redirection driver, installed in a volatile memory of the computer system upon power-up initialization, that when executed, is configured to:

automatically intercept a request to modify one of the designated locations or to modify a location referred to by the unprotected space table;

when the request is to modify a location referred to by the unprotected space table, disregard the request so that data in the location referred to by the unprotected space table is modified according to the request; and

when the request is to modify one of the designated locations,

use the protected space redirection table to determine whether the designated location has been previously redirected;

when it is determined that the designated location has been previously redirected,

determine an associated redirected location referred to by the protected space redirection table; and

redirect the request to the associated redirected location; and

when it is determined that the designated location has not been previously redirected,

allocate a new redirected location based on the available space table;

redirect the request to modify one of the designated locations to the new redirected location;

record a reference to the new redirected location in the protected space redirection table; and

remove the reference to the new redirected location from the available space table.

80. (Canceled)

81. (Previously Presented) The storage access redirection system of claim 79 wherein the redirection driver receives a request to read one of the designated locations and redirects the read request to an associated redirected location when it is determined that the designated location has been previously redirected.

82-83. (Canceled)

84. (Currently Amended) A method in a computer system for automatically protecting data stored in a portion of a storage device having a designated protected space, the computer system having a designated unprotected space and a redirected space, comprising:

loading a software redirection driver into an input/output driver hierarchy loaded in a volatile memory of the computer system during power-up initialization, wherein the software redirection driver is an input/output driver; and

under control of code of the loaded software redirection driver, redirecting input/output requests by:

intercepting from requesting code that is external to the loaded software redirection driver a request to modify a location referred to by a protected space redirection table or a location referred to by an unprotected space table;

when the request is to modify a location referred to by the unprotected space table, initiating modification of the location in the unprotected space without redirection;

when the request is to modify a location referred to by the protected space redirection table,

determining, based on the protected space redirection table, a location in the redirected space that is mapped to the location in the protected space; and

redirecting the intercepted request to modify the determined location in the redirected space instead of the location in the protected space, so that the data stored in the location in the protected space automatically remains unaltered when the computer system is restarted from a powered-down state.

85. (Previously Presented) The method of claim 84 further comprising:

when the request has not been previously redirected, allocating the location in the redirected space based on an available space table; and

recording in the protected space redirection table a reference to the location in the redirected space.

86. (Previously Presented) The method of claim 84 wherein the redirected space table maps locations in the protected space to locations in the redirected space.

87. (Previously Presented) The method of claim 86 wherein the locations in the protected space include at least one of a file, a sector, or a cluster.

88 (Previously Presented) The method of claim 84 wherein the unprotected space table includes indications of unprotected locations on the storage device.

89. (Previously Presented) The method of claim 88 wherein the unprotected locations include at least one of a file, a sector, or a cluster.

90. (Previously Presented) The method of claim 84 wherein the driver is inserted into a driver hierarchy that is controlled by an operating system of the computer system.

91. (Previously Presented) The method of claim 84 wherein the request to modify the location is a request to write a location in the protected space.

92. (Previously Presented) The method of claim 84 wherein at least one of the protected space, the unprotected space, or the redirected space are organized according to multiple storage abstractions.

93. (Currently Amended) A computer-readable memory medium containing program code that controls a computer processor to protect data stored in a portion of a storage device having a designated protected space, the computer system having a designated unprotected space and a redirected space, by performing a method comprising:

loading a software redirection driver into an input/output driver hierarchy loaded in a volatile memory of the computer system during power-up initialization, wherein the software redirection driver is an input/output driver; and

under control of code of the loaded software redirection driver, redirecting input/output requests by:

intercepting from requesting code that is external to the loaded software redirection driver a request to modify a location referred to by a protected space redirection table or a location referred to by an unprotected space table;

when the request is to modify a location referred to by the unprotected space table, initiating modification of the location in the unprotected space without redirection;

when the request is to modify a location referred to by the protected space redirection table,

determining, based on the protected space redirection table, a location in the redirected space that is mapped to the location in the protected space; and

redirecting the intercepted request to modify the determined location in the redirected space instead of the location in the protected space, so that the data stored in the location in the protected space automatically remains unaltered when the computer system is restarted from a powered-down state.

94. (Previously Presented) The computer-readable medium of claim 93 wherein the method further comprises:

when the request has not been previously redirected, allocating the location in the redirected space based on an available space table; and

recording in the protected space redirection table a reference to the location in the redirected space.

95. (Previously Presented) The computer-readable medium of claim 93 wherein the redirected space table maps locations in the protected space to locations in the redirected space.

96. (Previously Presented) The computer-readable medium of claim 95 wherein the locations in the protected space include at least one of a file, a sector, or a cluster.

97. (Previously Presented) The computer-readable medium of claim 93 wherein the unprotected space table includes indications of unprotected locations on the storage device.

98. (Previously Presented) The computer-readable medium of claim 97 wherein the unprotected locations include at least one of a file, a sector, or a cluster.

99. (Previously Presented) The computer-readable medium of claim 93 wherein the driver is inserted into a driver hierarchy that is controlled by an operating system of the computer system.

100. (Previously Presented) The computer-readable medium of claim 93 wherein the request to modify the location is a request to write a location in the protected space.

101. (Previously Presented) The computer-readable medium of claim 93 wherein at least one of the protected space, the unprotected space, or the redirected space are organized according to multiple different storage abstractions.